U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEES ON RESEARCH & TECHNOLOGY AND OVERSIGHT

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Friday, July 24 2015
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

Purpose

On Friday, July 24, 2015, the Research & Technology and Oversight Subcommittees will hold a joint hearing to discuss various industry best practices relative to cybersecurity, share lessons learned from the private sector, inform on how innovative private sector security practices can be applied to government agencies particularly in the wake of recent data breaches at the Office of Personnel Management (OPM), and address the effectiveness of voluntary federal standards for cybersecurity. The Science, Space, and Technology Committee previously held a hearing on July 8 titled, *Is the OPM Data Breach the Tip of the Iceberg?* [1] The Committee's jurisdiction includes the National Institute of Standards and Technology (NIST), which develops cybersecurity standards and guidelines,[2] the Department of Homeland Security's Science and Technology Directorate (DHS S&T) and research and development related to cybersecurity at the National Science Foundation (NSF).

Witnesses

- **Mr. John B. Wood**, Chief Executive Officer and Chairman, Telos Corporation
- **Dr. Martin Casado**, Senior Vice President and General Manager, Networking and Security Business Unit, VMWare
- **Mr. Ken Schneider**, Vice President of Technology Strategy, Symantec Corporation
- **Mr. Larry Clinton**, President and Chief Executive Officer, Internet Security Alliance

Background

On June 4th, 2015, OPM announced that it had identified a cyber-breach affecting personnel data for approximately 4 million current and former federal employees, including personally identifiable information (PII).[3] Later that month, OPM reported a separate cyber

[1] Hearing information found at: http://science.house.gov/hearing/subcommittee-research-and-technology-and-subcommittee-oversight-hearing-opm-data-breach-tip

[2] As authorized by the Federal Information Security Management Act (FISMA) of 2002, enacted as Title III of the E-Government Act (Public Law 107-347) in December 2002, found at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. NIST's responsibilities for cybersecurity were last updated in the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) found at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf and Federal Information Security Modernization Act (P.L. 113-283) found at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

[3] https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/

incident targeting OPM's databases housing background investigation records, and announced on July 9th that an investigation concluded that the information of an additional 19.7 million individuals that applied for a background investigation had been stolen. The combined breaches are estimated to have compromised the sensitive information of 21.5 million individuals.[4]

The OPM breaches highlight the growing challenges of cybersecurity for both the public and private sector, as the number of cyber threats to both has grown exponentially in recent years. According to the U.S. Government Accountability Office (GAO), the number of information security incidents reported by federal agencies to US-CERT (the U.S. Computer Emergency Readiness Team, part of the Department of Homeland Security) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 – an increase of over 1000 percent.[5]

A 2014 survey of private companies found that the number of detected incidents rose to 42.8 million, a 48% increase over 2013. The survey also found that the total financial losses attributed to security compromises increased 34% over 2013.[6] The impact to individual Americans grows too, as an estimated 12.7 million Americans experienced some sort of financial identity theft in 2014, costing $16 billion in financial losses.[7] In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, J.P. Morgan-Chase, Sony Pictures, and Anthem Health Insurance were only a few of the many publicly disclosed breaches.[8] The data breach of Anthem alone exposed the social security numbers of nearly 80 million Americans.

Federal Cybersecurity Laws and Regulations

The federal role in cybersecurity involves both security for federal systems and assisting in protecting nonfederal systems. More than 50 federal statutes address various aspects of cybersecurity. These include:

Federal Information Security Management Act

The cybersecurity of federal systems is governed by the Federal Information Security Management Act, which was last updated by the Federal Information Security Modernization Act (P.L. 113-283) in December 2014. FISMA created a security framework for federal information systems, with an emphasis on risk management, and gave specific responsibilities to the Office of Management and Budget (OMB), National Institutes of Standards and Technology

[4] https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

[5] *Actions Needed to Address Challenges Facing Federal Systems*, GAO-15-573T, April 22, 2015. Available at: http://www.gao.gov/products/GAO-15-573T

[6] The Global State of Information Security Survey 2015. Available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

[7] http://www.nbcnews.com/business/consumer/nearly-13-million-americans-victimized-id-thieves-2014-n316266

[8] 2014: A Year of Mega Breaches, Ponemon Institute, 1, (January 2015). Available at http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf

(NIST), and the heads, chief information officers (CIOs), chief information security officers (CISOs), and inspectors general (IGs) of federal agencies.[9]

FISMA makes OMB responsible for overseeing federal information-security policy, evaluating agency programs, and promulgating cybersecurity standards developed by NIST. Each agency must designate an information-security officer, with responsibilities including agency-wide programs, policies, and procedures, training of security and other personnel, processes for remedial action to address deficiencies, and procedures for handling security incidents and ensuring continuity of operations. Agencies must also develop performance plans, conduct independent annual evaluations of their cybersecurity programs and practices, and provide annual reports on compliance and effectiveness to Congress. FISMA requirements also apply to contractors who run information systems on behalf of an agency.[10]

Cybersecurity Enhancement Act of 2014

In December 2014, the *Cybersecurity Enhancement Act of 2014* (P.L. 113-274) passed the House and Senate and was signed into law. The law strengthens the efforts of NSF and NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development. P.L. 113-274 coordinates research and related activities conducted across Federal agencies to better address evolving cyber threats.

Executive Order 13636 on Improving Critical Infrastructure and Framework for Improving Critical Infrastructure Cybersecurity

In February 2013, President Obama issued an executive order (EO) on cybersecurity for critical infrastructure.[11] Among other provisions, the EO encouraged information sharing between public and private sectors and directed NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST was instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework.

In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* in response to the EO. NIST worked in collaboration with industry stakeholders to establish a three-pronged framework that includes a Core, Profile, and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[12]

[9] *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137, October 2011, http://www.gao.gov/new.items/d12137.pdf
[10] *Cybersecurity: FISMA Reform*, CRS Insights, December 15, 2014.
[11] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[12] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf